INTRODUCTION TO CRYPTOGRAPHY
(CSEN 3239)

Time Allotted : 2½ hrs **Full Marks : 60**

Figures out of the right margin indicate full marks.

Candidates are required to answer Group A and any 4 (four) from Group B to E, taking one from each group.

Candidates are required to give answer in their own words as far as practicable.

Group – A

1. Answer any twelve: **12 × 1 = 12**

Choose the correct alternative for the following

(i) SHA-1 produces a hash value of
(a) 256 bits (b) 160 bits
(c) 180 bits (d) 124 bits

(ii) Find 3^{201} mod 11 =
(a) 3 (b) 5 (c) 6 (d) 10

(iii) On Encrypting "cryptography" using Vignere Cipher System using the keyword "LUCKY" we get cipher text
(a) nlazeiibljji (b) nlazeiibljii
(c) olaaeiibljki (d) mlaaeiibljki

(iv) Public key cryptography is advantageous over Symmetric key Cryptography due to
(a) speed (b) space
(c) key exchange (d) key length

(v) Suppose that everyone in a group of N people wants to communicate secretly with the N-1 others using symmetric key cryptographic system. The communication between any two persons should not be decodable by the others in the group. The number of keys required in the system as a whole to satisfy the confidentiality requirement is
(a) 2N (b) N(N-1) (c) N(N-1)/2 (d) $(N-1)^2$

(vi) An attack on a cipher text message where the attacker attempts to use all possible permutations and combinations is called:
(a) Brute-Plaintext attack (b) Birthday attack
(c) Known-Plaintext attack (d) Chosen-plaintext attack.

(vii) In the DES algorithm the round key is _____ bits and the Round Input is _____ bits.
(a) 48, 32 (b) 64,32 (c) 56, 24 (d) 32, 32

(viii) Which algorithm is susceptible to Bucket Brigade attack?
(a) Diffie-Hellman (b) Double DES
(c) Triple DES (d) RSA

(ix) How can we avoid man-in-the-middle attacks?
(a) Accept every SSL certificate, even the broken ones.
(b) Use connections without SSL.
(c) Use HTTPS connections and verify the SSL certificate.
(d) None of the above.

(x) The Authentication Header (AH) protocol, part of IPSec, provides which of the following security functions?
(a) Source authentication
(b) Data integrity
(c) Data confidentiality
(d) Source authentication and data integrity.

Fill in the blanks with the correct word

(xi) In the digital signature technique, the sender of the message uses_____ to create the cipher text.

(xii) In cryptography, the order of the letters in a message is rearranged by _____.

(xiii) IPSec services are available in _____ layer.

(xiv) When two different message-digests have the same value, it is called _____.

(xv) The minimum positive integer p such that 3p modulo 17 = 1 is_____.

Group - B

2. (a) Explain Fermat's theorem with proper example. *[(CO2)(Remember/LOCQ)]*
(b) Evaluate gcd(1547,560) using Euclid's algorithm. Define Euler's totient function and its application. *[(CO2)(Evaluate/IOCQ)]*
(c) Find multiplicative inverse of 5 mod 11 using Fermat's theorem. *[(CO2)(Apply/LOCQ)]*

3 + 6 + 3 = 12

3. (a) Find 8^{-1}mod 77 (multiplicative inverse) using Euler's theorem? *[(CO2)(Apply/IOCQ)]*
(b) Solve x =3(mod 5), x=1(mod 7), x=6(mod 8) using Chinese Remainder Theorem. *[(CO1,CO2)(Remember/LOCQ)]*
(c) How many primate roots are there in modulo 7 and modulo 11? 2 is a primitive root modulo 13. What are the other primitive roots modulo 13? *[(CO2)(Remember/LOCQ)]*

3 + 5 + (2 + 2) = 12

Group - C

4. (a) Discuss principles of security. *[(CO1)(Remember/LOCQ)]*
(b) Explain HMAC algorithm with suitable diagram. *[(CO4)(Remember/LOCQ)]*

(c) Discuss the pros and cons of symmetric and asymmetric key cryptography. *[(CO1)(Understand/LOCQ)]*

3 + 6 + 3 = 12

5. (a) Encrypt the message " COMSEC means communications security" with the key word "GALOIS" using Polygraphic Substitution Ciphers (Playfair Cipher). *[(CO5,CO1)(Analyse/HOCQ)]*

(b) Decrypt the message "TRLEELIGCIGEHALANTNCTECYENEN" with the keyword "ANALYST" using simple columnar transposition technique. *[(CO5,CO1)(Understand/LOCQ)]*

(c) Explain the following algorithm modes with neat diagram: (i) Electronic code book mode (ii) Cipher block chaining mode. *[(CO3)(Explanation/IOCQ)]*

4 + 2 + 6 = 12

Group - D

6. (a) Explain the Diffie-Hellman Key Exchange Algorithm. Alice and Bob want to establish a secret key using the Diffie-Hellman Key Exchange Algorithm. Assuming the values as q = 11 and a primitive root alpha=7, find out the values of the secret keys K1 and K2. *[(CO5)(Evaluate /HOCQ)]*

(b) Explain man in the middle attack with a suitable example. *[(CO5)(Analyze/LOCQ)]*

(c) What do you mean by Public key Cryptosystem? *[(CO4)(Remember/IOCQ)]*

5 + 5 + 2 = 12

7. (a) Given p=17, q=11, and e=7 use RSA algorithm to find n, d, Public and Private Key. *[(CO4,CO5)(Evaluate/HOCQ)]*

(b) Explain ElGamal public key cryptosystem. *[(CO4)(Remember/LOCQ)]*

(c) What is the key distribution problem? *[(CO5)(Understand/LOCQ)]*

6 + 5 + 1 = 12

Group - E

8. (a) Write an algorithm to generate a digital signature using the RSA algorithm *[(CO4)(Remember/LOCQ)]*

(b) State the possible attacks on RSA signature. *[(CO5)(Remember/LOCQ)]*

(c) State how DSA can be used to generate the digital signature. *[(CO4)(Apply/IOCQ)]*

5 + 3 + 4 = 12

9. (a) Differentiate between transport and tunnel modes of operation of IPSec. *[(CO6)(Understand/LOCQ)]*

(b) Write a short note on Intrusion Detection. *[(CO6)(Remember/LOCQ)]*

(c) Discuss General IPSec ESP packet format. *[(CO6)(Remember/LOCQ)]*

4 + 4 + 4 = 12

Cognition Level	LOCQ	IOCQ	HOCQ
Percentage distribution	62.5	21.87	15.63

Course Outcome (CO):

After the completion of the course students will be able to

CSEN3239.1 Understand OSI security architecture and classic encryption techniques.

CSEN3239.2 Acquire fundamental knowledge on the concepts of finite fields and number theory.

CSEN3239.3 Understand various block cipher and stream cipher models.

CSEN3239.4 Describe the Principles of public key cryptosystems, hash functions and digital signature.

CSEN3239.5 Learn about various cryptographic techniques, which include private and public keys algorithms along with attacks types.

CSEN3239.6 Understand authentication requirements and study various authentication mechanisms.

**LOCQ: Lower Order Cognitive Question; IOCQ: Intermediate Order Cognitive Question; HOCQ: Higher Order Cognitive Question.*